Security Incident Reporting Criteria

Carrianne J. Zimmerman

Office of Security Enforcement

Office of Enforcement and Oversight

March 27, 2012

Overview

- What's Different
- Categorization
- Reporting
- Conduct of Inquiry
- Incident Closeout
- Challenges – Enforcement Coordinator

What's Different

- DOE Order 470.4B, Attachment 5, Section 1
- Incident Categorization
- Notification and Reporting
- Inquiry and Closeout

Categorization

- Significance Level Category A
  - Meets a designated level of significance relative to the potential impact on the Department and/or national security
  - Notification to DOE/NNSA Cognizant Security Office and contractor Cognizant Security Office
  - DOE/NNSA Cognizant Security Office involvement imperative for assessing impacts, coordinating with external agencies, and notifying senior management

Categorization (cont'd)

- Significance Level Category B
  - Less significant incidents that do not meet Category A significance criteria
  - Notification to contractor Cognizant Security Office
  - Does not preclude DOE/NNSA Cognizant Security Office oversight responsibilities
  - Monitoring of B incidents by contractor is essential to proactively address recurring incidents

Categorization (cont'd)

- Significance Level Type
  - Security Interest – Involves the loss, theft, compromise, or suspected compromise of Departmental assets (all classified information)
  - Management Interest – Warrants management notification only
  - Procedural Interest – Failure to follow procedures, and all evidence suggests classified assets were not compromised or the likelihood of compromise is remote

Reporting

- Timeframe - Maximum 5 calendar days to conduct preliminary inquiry and make initial categorization and notification
- Category A incidents – Reported in the Safeguards and Security Information Management System (SSIMS)
- Category B incidents – Optional reporting in SSIMS or reported in a local tracking system

Conduct of Inquiry

- Office of Health, Safety and Security Development of DOE Technical Standard – Incidents of Security Concern
- Contractor Incidents of Security Concern Program Plan
- Supporting Documented Evidence

Incident Closeout

- Category A Incidents
  - 90 calendar days from notification
  - Closed in SSIMS
- Category B Incidents
  - Closed in SSIMS or,
  - Closed in a local tracking system

Challenges – Enforcement Coordinator

- Understand the New Policy and the Potential Regulatory Concerns
  - Potentially less reporting to Headquarters
  - More reliance on local trending activities
- Focus on Significant Incidents and also be aware of Incident Trends
  - Performance precursors – less significant incidents
  - Proactive not reactive

Challenges – Enforcement Coordinator (cont'd)

- Be Actively Involved in the Development of the Contractor Incidents of Security Concern Program Plan
  - Establishes Contractor processes for identification, notification, reporting, and trending of classified information security noncompliances
  - Integrate Coordinator involvement

Challenges – Enforcement Coordinator (cont'd)

- Be Aware and Actively Involved in Voluntary Reporting of Regulatory Concerns
  - Timely and accurate reporting
  - Transparency
  - Potential mitigation

Questions?